Privacy - Regolamento UE - Studio professionista - nozioni generali - misure di sicurezza - notifica di violazione

Per la privacy, non essendovi innovazioni sostanziali, si ritiene di poter rammentare le nozioni generali e le definizioni nel seguente modo schematico.

ambito di applicazione	dati di persone fisiche	esclusi i restanti soggetti
dato personale	qualsiasi informazione relativa ad una persona fisica	identificata o identificabile direttamente o indirettamente (anche con un identificativo online)
dati personali ***"sensibili"***	• origine razziale o etnica • opinioni politiche * • convinzioni religiose * • convinzioni filosofiche * • appartenenza sindacale • dati genetici e biometrici che consentano l'identificazione univoca • dati relative allo stato di salute * • dati relative alla vita sessuale od orientamento sessuale *	trattamento con **consenso scritto** dell'interessato *dove" rilevo tali dati: schede 8 - 5 - 2 per mille, doc. relativa alla dich. redditi (quadro RP, doc. spese sanitarie, erogazioni ad onlus etc.) - documentazione attestante stati di salute nel corso di accertamenti o di acc.ti con adesione etc.
dati *"riservati"*	nei dati sensibili non sono compresi quelli relative a: • redditi • patrimoni • investimenti • numeri di telefono cellulare etc.	questi dati non sono *"regolamentati"*, in quanto l'eventuale divulgazione non compromette nè i diritti nè le libertà fondamentali della persona - sono dati comunque da tutelare, anche ai fini del rispetto dell'obbligo del segreto professionale
trattamento dei dati	qualsiasi operazione, quale	• **consultazione**

	• raccolta • registrazione • organizzazione • strutturazione • conservazione • adattamento e/o modifica • distruzione • estrazione	• uso • comunicazione mediante trasmissione • raffronto • interconnessione • limitazione • cancellazione
principi nel trattamento dei dati	• liceit • finalità determinate • dati adeguati , pertinenti e limitati rispetto alle finalità • dati esatti ed aggiornati • conservazione limitata alle finalità • trattati con adeguata sicurezza	

MISURE DI SICUREZZA NEL TRATTAMENTO - notifica di violazione

Il Regolamento, è ovvio, a differenza del D.lgs. 196/2003 (art. 33-36 e allegato B), non indica alcuna specifica misura di sicurezza da adottare.
Gli obblighi in materia di sicurezza dei dati posti a carico del titolare del trattamento sono riscontrabili nei seguenti punti del Regolamento:

sicurezza dei dati - art. 5 protezione mediante procedure tecniche e organizzative adeguate, da trattamenti non autorizzati od illeciti, dalla perdita, distruzione o dal danno accidentale (integrità dei dati)	il titolare del trattamento è competente su tali aspetti e in grado di comprovarlo	quindi nella valutazione del rischio - o altro documento - occorrerà indicare quali siano i rischi e le conseguenti misure tecniche ed organizzative adottate
responsabilità - art. 24 tenuto conto del rischio, della natura dei dati etc. il titolare mette in atto misure tecniche ed organizzative adeguate	...e deve essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento	come sopra, oltre che "tali misure sono riesaminate e aggiornate qualora necessario"
sicurezza - art. 32 misure di sicurezza adeguate al rischio	misure atte a garantire: • riservatezza (divulgazione, accessi non autorizzati etc.) • integrità (perdita, distruzione dei dati o di parte di essi) • ripristino dei dati in caso	come sopra

	di incidente fisico o tecnico	
obbligo di notifica di violazione all'autorità di controllo (art. 33)	in caso di violazione dei dati personali il titolare del trattamento deve notificare la violazione all'autorità di controllo	senza ingiustificato ritardo e se possibile entro 72 ore - qualora effettuata oltre tlae termine è corredata dai motivi del ritardo
obbligo di notifica di violazione all'interessato	nel caso di rischio elevato per i diritti e le libertà delle persone fisiche - senza ingiustificato ritardo	esonero nel caso di: • cifratura dei dati • adozione successiva di misure atte a scongiurare il sopraggiungere di un rischio elevato • la comunicazione richiederebbe sforzi sproporzionati L'Autorità di Controllo può richiedere al titolare di effettuare la notifica all'interessato (a seguito della notifica di cui al punto precedente)

Le misure di sicurezza da adottare

Si ritiene che, considerata anche la natura del rischio, un *"normale"* studio di commercialista debba valutare/adottare le seguenti misure di sicurezza, desunte da una *"standardizzazione"* dei rischi riscontrabili negli studi, sottolineando comunque che la valutazione del rischio è un "abito su misura" e non può essere "preconfezionato", variando le condizioni di operatività da studio a studio.

accesso ai locali dello studio - valutazione	in considerazione dell'ubicazione dello studio (es. impianto di allarme) - eventuale distanza di cortesia al bancone della reception
accesso agli archivi "cartacei"	appositi locali (non ad esempio cartelline e scaffali con dossier anche nei servizi) - porta chiusa dell'archivio - cartello riportante l'avviso di accesso consentito solo a personale autorizzato
uffici ove hanno accesso i Clienti	la copertina delle cartelline "visibili" (quelle sulla scrivania) dovrebbe riportare esclusivamente il nominativo del cliente - non l'oggetto della pratica, non numeri di telefono etc. che andrebbero indicate

	all'interno della cartellina
distruggi documenti e distruzione dei documenti prima di inserirli nel contenitore della raccolta differenziata	anche fini del rispetto del segreto professionale
collocazione dei sistemi informatici	rialzati da terra, ad evitare danni derivanti da possibili dispersioni di acqua e/o altre sostanze
collocazione del server	in locale non accessibile ai clienti - preferibilmente in apposito armadio rack
memorizzazione dei dati	esclusivamente sul server, in modo che sia garantito puntualmente il salvataggio dei dati - vedi anche la voce Gruppo di Continuità
schermi degli strumenti informatici	non orientati in modo che siano visibili dai Clienti (fatto salvo lo schermo che serve a proiettare diapositive relative alla pratica, bozza della scrittura o dell'atto da stipulare etc.)
accesso agli strumenti informatici	username e password -almeno di 8 caratteri preferibilmente alfanumerici - da variare almeno ogni 3 mesi
aggiornamento delle "patches" (ad esempio gli aggiornamenti delle versioni di Windows)	impostazione automatica sui p.c.
Programma antivirus *	impostazione di aggiornamento automatico giornaliero o al rilascio di aggiornamenti
gruppo di continuità	installazione per il solo server (considerato quanto indicato al punto Memorizzazione dei dati)
firewall *	impostazione da parte dell'assistenza hardware - software
salvataggio e back up *	impostazione a carico dell'assistenza hardware - software consigliabile il salvataggio giornaliero (all. B al D.lgs. almeno settimanale)

salvataggio - supporti	custodia di eventuali supporti di salvataggio dei dati in luogo sicuro (ad es. cassaforte - oppure contenitore ignifugo etc.)
ripristino dei dati *	da parte dell'assistenza hardware-software
supporti rimovibili	uso sconsigliato di chiavette USB etc. - necessitano di istruzioni organizzative e tecniche per la custodia e l'uso
Per i punti contrassegnati da *, considerato che tali misure sono affidate alla ditta di assistenza hardware - software, questa rilascerà apposita dichiarazione di conformità dei dispositivi e del corretto funzionamento degli stessi.	

Si rammenta che:

- il D.lgs. 231/2007 in materia di **antiriciclaggio** dispone che
  art. 16 c. 4 - I sistemi e le procedure adottati ai sensi del presente articolo rispettano le prescrizioni e garanzie stabilite dal presente decreto e dalla normativa vigente in materia di protezione dei dati personali

- *art. 32 c. 1 - I soggetti obbligati adottano sistemi di conservazione dei documenti, dei dati e delle informazioni idonei a garantire il rispetto delle norme dettate dal codice in materia di protezione dei dati personali nonché il trattamento dei medesimi esclusivamente per le finalità di cui al presente decreto*

- qualora si intenda attivare un sistema di **videosorveglianza** occorre che preliminarmente all'installazione vi sia il parere favorevole delle rappresentanze sindacali e, ove non esistenti, l'autorizzazione all'Ispettorato del Lavoro (**vedi il provvedimento del Garante**).

Sul cartello-informativa che segnala la presenza delle telecamere è opportuno riportare il numero di autorizzazione rilasciata dall'Ispettorato del Lavoro.